<u>Amendments to the Claims:</u>

This listing of claims will replace all prior versions, and listings, of claims in the application:

<u>Listing of Claims:</u>

1. (Currently Amended) A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, <u>and at least one computer including</u> an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:

    a.   a user registration step, wherein a user registers with an electronic identicator at least one registration biometric sample taken <u>via a biometric sensor</u> directly from the person of the user;

    b.   formation of a rule module customized to the user in a rule module clearinghouse, wherein at least one pattern data of a user is ~~associated~~ <u>stored in the computer in association</u> with at least one execution command of the user;

    c.   a user identification step, wherein the electronic identicator compares a bid biometric sample <u>subsequently</u> taken directly from the person of the user <u>via a biometric sensor</u> with at least one previously registered biometric sample for producing either a successful or failed identification of the user;

    d.   a command execution step, wherein upon successful identification of the user at least one previously designated rule module of the user is invoked <u>by the electronic rule module clearinghouse</u> to execute at least one electronic transmission;

wherein a biometrically authorized electronic transmission is conducted without the user presenting smartcards or magnetic swipe cards.

2. (Currently Amended) The method of claim [[1]] <u>1,</u> wherein during the command execution step, the electronic rule module clearinghouse communicates with one or more third-party computers.

3. (Currently Amended) The method of claim [[1]] 1, wherein said execution commands are comprised of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules.

4. (Currently Amended) The method of claim [[1]] 1, wherein pattern data comprises one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, Internet browsing patterns, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature.

5. (Previously Presented) The method of claim 1, wherein pattern data for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

6. (Previously Presented) The method of claim 1, wherein an execution command for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

7. (Currently Amended) The method of claim [[1]] 1, further comprising a user re-registration check step, wherein the user's registration biometric sample is compared against previously registered biometric samples wherein if a match occurs, the computer system is alerted to the fact that the user has attempted to re-register with the electronic identicator.

8. (Currently Amended) The method of claim [[1]] 1, wherein the biometric sample comprises one or more of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print.

9.   (Currently Amended) The method of claim [[1]] 1, wherein during the identification step, the user provides a personal identification code to the electronic identicator along with a bid biometric sample for purposes of identifying the user.

10.   (Currently Amended) The method of claim [[9]] 9, further comprising a biometric theft resolution step, wherein a user's personal identification code is changed when the user's biometric sample is determined to have been fraudulently duplicated.

11.   (Original) The method of claim 1, wherein execution of an execution command authorizes the user to access stored electronic data.

12.   (Currently Amended) The method of claim [[11]] 11, wherein accessing stored electronic data results in activation of an Internet-connected device.

13.   (Currently Amended) The method of claim [[1]] 1, wherein executing an execution command processes electronic data to provide the user with a user requested electronic transmission.

14.   (Previously Presented) The method of claim 13, wherein said processing comprises invoking one or more of the following: a user's digital certificate, a user's identity scrambler, a user's interactive electronic consumer loyalty or consumer rewards program, a user's interactive electronic advertising, a user's interactive instant messaging program, a user's email authentication, and an automated electronic intelligent agent for electronic data search and retrieval that is customized to the user's requests.

15.   (Currently Amended) The method of claim [[1]] 1, wherein executing an execution command presents electronic data that is customized to the user's requested electronic transmission.

16.   (Currently Amended) The method of claim [[1]] 1, further comprising a user log-in repeat step, wherein during an electronic transmission the user is periodically required by the electronic identicator to present the user's bid biometric sample or at least one of the user's pattern data.

17.   (Currently Amended) The method of claim [[1]] 1, further comprising a communications step wherein one or more of the following is used: the Internet, an intranet, an extranet, a local area network, and a wide area network.

18.   (Currently Amended) The method of claim [[1]] 1, further comprising a third-party registration step, wherein a third-party registers identification data with the electronic identicator, the identification data comprising one or more of the following: a biometric, a digital certificate, an Internet protocol address, and a biometric input apparatus hardware identification code.

19.   (Currently Amended) The method of claim [[18]] 18, further comprising a third-party identification step, wherein a third-party providing the user with electronic transmissions is identified by the electronic identicator by comparing the third-party's bid identification data with the third-party's registered identification data.

20.   (Previously Presented) A computer system device for tokenless biometric processing of electronic transmissions, using at least one user biometric sample, an electronic identicator and an electronic rule module clearinghouse, comprising:

a.   a biometric input apparatus, for providing a bid or registration biometric sample of a user to the electronic identicator, wherein a user registers with an electronic identicator at least one registration biometric sample taken directly from the person of the user;

b.   an electronic rule module clearinghouse, having at least one rule module further comprising at least one pattern data of the user associated with at least one execution command of the user, for executing at least one electronic transmission;

c.   an electronic identicator, for comparing the bid biometric sample with registered biometric samples of users;

d.   a command execution module, for invoking at least one previously designated execution command in the electronic rule module clearinghouse to execute an electronic transmission;

wherein no smartcards or magnetic swipe cards are presented by the user to conduct the electronic transmission.

21. (Currently Amended) The device of claim [[20]] 20, wherein the command execution module communicates with one or more third-party computers.

22. (Currently Amended) The device of claim [[20]] 20, wherein pattern data comprises one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature.

23. (Previously Presented) The device of claim 20, wherein pattern data for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

24. (Previously Presented) The device of claim 20, wherein an execution command for a user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

25. (Currently Amended) A tokenless biometric method for processing electronic transmissions, using at least one user biometric sample, and at least one computer including an electronic identicator and an electronic rule module clearinghouse, said method comprising the steps of:

    a. a primary and subordinated user registration step, wherein a primary and subordinated user each register with an electronic identicator at least one registration biometric sample taken directly from the person of the primary and subordinated user via a biometric sensor, respectively;

    b. formation of a rule module customized to the primary and subordinated user in a rule module clearinghouse, wherein at least one pattern data of the primary and subordinated user is ~~associated~~ stored in the computer in association with at least one execution command of the primary and subordinated user, the rule module customized to the

primary user is customizable by the primary user and the rule module customized to the subordinated user is customizable by the subordinated user;

c.   a subordinated user identification step, wherein the electronic identicator compares a bid biometric sample taken directly from the person of the subordinated user <u>via a biometric sensor</u> with at least one previously registered biometric sample for producing either a successful or failed identification of the subordinated user;

d.   a subordination step wherein upon successful identification of the subordinated user, the pattern data of the subordinated user is searched to determine if any of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules; and

e.   a command execution step, wherein upon the successful identification of the subordinated user and the determination that at least one of the subordinated user's rule modules is subordinated to at least one of the primary user's rule modules, at least one previously designated execution command of the primary user is invoked <u>by the electronic rule module clearinghouse</u> to execute at least one electronic transmission;

wherein a biometrically authorized electronic transmission is conducted without the primary and subordinated user presenting smartcards or magnetic swipe cards.

26.   (Currently Amended) The method of claim [[3]] <u>3,</u> wherein execution commands for accessing stored electronic data include permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products ~~like alcohol and tobacco~~; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

27.   (Currently Amended) The method of claim [[26]] <u>26,</u> wherein accessing insurance benefits further comprises validating a user's health insurance benefits to permit admission to a hospital.

28.   (Currently Amended) The method of claim [[26]] <u>26,</u> wherein accessing membership benefits further comprises one or more of the following: validating a user's eligibility to rent videos under their pre-paid membership; validating a user's eligibility to

access an Internet web site; and validating a user's eligibility to enter a real-time internet chat room with other people on-line.

29. (Currently Amended) The method of claim [[26]] 26, wherein accessing event admittance further comprises one or more of the following: validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-rated film being shown in theatres; and validating a user's eligibility to board a vehicle of travel.

30. (Currently Amended) The method of claim [[11]] 11, wherein accessing stored electronic data comprises accessing one or more of the following: word-processing files; spreadsheet files; software code; graphics files; audio files; medical records; internet web sites; on-line audio or graphical content; electronic game content; on-line chat content; on-line messaging content; on-line educational content; on-line academic examination-taking; on-line personalized medical and health content; and server-based computer software programs and hardware drivers.

31. (Currently Amended) The method of claim [[1]] 1, wherein at least one rule module further comprises one or more of the following: at least one pattern data associated with at least two execution commands; and at least one execution command associated with at least two pattern data.

32. (Currently Amended) The method of claim [[12]] 12, wherein activation of an internet Internet-connected device further comprises activating one or more of the following devices: a wireless pager; a wireless telephone; a network computer; an exercise machine; a television; an electronic book; a radio; a household appliance; a personal digital assistant; a photocopy machine; and a digital audio player.

33. (Currently Amended) The method of claim [[14]] 14, wherein the automated intelligent agent for electronic data search and retrieval further comprises conducting periodic, user-customized on-line retrievals for one or more of the following data: medical updates; pending Internet auctions; electronic stock trades; e-mails; instant messages; voice over internet phone calls; electronic advertisements; and faxes.

34.   (Currently Amended) The method of claim [[29]] 29, wherein the vehicle of travel further comprises one or more of the following: an airplane; a train; a boat; and a bus.

35.   (Currently Amended) The method of claim [[14]] 14, wherein the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future.

36.   (Currently Amended) The method of claim [[14]] 14, wherein invoking a user's digital certificate with an electronic transmission to verify the authenticity of the sender and the electronic document's contents to yield a secure, authenticated electronic transmission.

37.   (Currently Amended) The method of claim [[13]] 13, wherein the processing of electronic transmissions further comprises execution commands which filter the access and presentation of data when the user is subordinated user.

38.   (Currently Amended) The method of claim [[37]] 37, wherein the filter governs subordinated user access to one or more of the following: Internet web sites with adult content; Internet sites with violent content; on-line session length; and educational on-line resources which are automatically "pushed" provided to the subordinated user during a particular on-line session, as pre-determined by the primary user.

39.   (Currently Amended) The device of claim [[20]] 20, wherein the execution commands for command includes accessing stored electronic data include including permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

40.   (Currently Amended) The device of claim [[39]] 39, wherein accessing insurance benefits further comprises validating a user's health insurance benefits to permit admission to a hospital.

41.   (Currently Amended) The device of claim [[39]] 39, wherein accessing membership benefits further comprises one or more of the following: validating a user's eligibility to rent videos under their pre-paid membership; validating a user's eligibility to access an Internet web site; and validating a user's eligibility to enter a real-time internet chat room with other people on-line.

42.   (Currently Amended) The device of claim [[39]] 39, wherein accessing event admittance further comprises one or more of the following: validating a user's eligibility to attend a music concert; validating a user's eligibility to attend a restricted event such as an R-rated film being shown in theatres; and validating a user's eligibility to board a vehicle of travel.

43.   (Currently Amended) The device of claim [[20]] 20, wherein execution commands further comprise accessing one or more of the following stored electronic data: word-processing files; spreadsheet files; software code; graphics files; audio files; medical records; internet web sites; on-line audio or graphical content; electronic game content; on-line chat content; on-line messaging content; on-line educational content; on-line academic examination-taking; on-line personalized medical and health content; and server-based computer software programs and hardware drivers.

44.   (Currently Amended) The device of claim [[20]] 20, wherein at least one rule module further comprises one or more of the following: at least one pattern data associated with at least two execution commands, and at least one execution command associated with at least two pattern data.

45.   (Currently Amended) The device of claim [[20]] 20, wherein execution commands further comprise activation of one or more of the following Internet-connected devices: a wireless pager; a wireless telephone; a network computer; an exercise machine; a television; an electronic book; a radio; a household appliance; a personal digital assistant; a photocopy machine; and a digital audio player.

46.   (Currently Amended) The device of claim [[20]] 20, wherein execution commands further comprise an automated intelligent agent for electronic data search and retrieval which conducts periodic, user-customized on-line retrievals for one or more of the following data: medical updates; pending Internet auctions; electronic stock trades; e-mails; instant messages; voice over internet phone calls; electronic advertisements; and faxes.

47.   (Currently Amended) The device of claim [[42]] 42, wherein the vehicle of travel further comprises one or more of the following: an airplane; a train; a boat; and a bus.

48.   (Currently Amended) The device of claim [[46]] 46, wherein the automated intelligent agent can extrapolate from the user's existing preferences and on-line activity patterns to automatically and periodically recommend to the user new data that may expand and delete the user's pattern data and execution commands based upon the intelligent agent's algorithmic projection of what the user's on-line preferences and activities will be in the future.

49.   (Currently Amended) The device of claim [[20]] 20, wherein execution commands further comprise invoking a user's digital certificate with an electronic transmission to verify the authenticity of the sender and the electronic document's contents to yield a secure, authenticated electronic transmission.

50.   (Currently Amended) The device of claim [[20]] 20, wherein execution commands further comprise the processing of electronic transmissions which filter the access and presentation of data when the user is a subordinated user.

51.   (Currently Amended) The device of claim [[50]] 50, wherein the filter governs subordinated user access to one or more of the following: Internet web sites with adult content; Internet sites with violent content; on-line session length; educational on-line resources which are automatically "pushed" provided to the subordinated user during a particular on-line session, as pre-determined by the primary user.

52.   (Currently Amended) The method of claim [[4]] 4, wherein said execution commands are comprised of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules.

53.   (Currently Amended) The method of claim [[53]] 52, wherein execution commands for accessing stored electronic data include permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

54.   (Currently Amended) A biometric method implemented in a computer system for processing electronic transmissions, comprising:
          registering in the computer system at least one registration biometric sample taken directly from a user via a biometric sensor;
          forming a rule module customized to the user in a rule module clearinghouse stored in the computer system, the rule module associating at least one pattern data of the user with at least one execution command of the user;
          comparing a bid biometric sample subsequently taken directly from the person of the user via a biometric sensor with at least one previously registered biometric sample for producing either a successful or failed match; and
          invoking the rule module of the user upon a successful match to execute at least one electronic transmission from the computer system.

55.   (Previously Presented) The method of claim 54, wherein the electronic transmission is executed without the user presenting smartcards or magnetic swipe cards.

56.   (Previously Presented) The method of claim 54, wherein registering at least one registration biometric sample includes:
          registering a plurality of biometric samples from a plurality of users; and
          basketing a subset of the plurality of samples to facilitate the comparison with the bid biometric sample.

57.   (Currently Amended) The method of claim 54, wherein comparing a bid biometric sample includes comparing the bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed identification of the user and invoking the rule module of the user includes locating the rule module customized to the user based on the identification of the user.

58.   (Previously Presented) The method of claim 54, wherein:

the execution command includes of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules; and

the execution command for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

59.   (Currently Amended) The method of claim 54, wherein the execution command includes permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products like alcohol and tobacco; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

60.   (Previously Presented) The method of claim 59, wherein:

the pattern data includes one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, Internet browsing patterns, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature; and

the pattern data for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

61.   (Previously Presented) The method of claim 54, wherein:

the pattern data includes one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, Internet browsing patterns, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature; and

the pattern data for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

62.   (Previously Presented) The method of claim 54, wherein:

the pattern data includes demographic information of the user; and

the execution command includes accessing stored electronic data to determine eligibility to purchase restricted products or to access data or services.

63.   (Currently Amended) A biometric method implemented in a computer system for processing electronic transmissions, comprising:

registering in the computer system at least one primary registration biometric sample taken via a biometric sensor directly from a primary user;

registering at least one secondary registration biometric sample taken via a biometric sensor directly from a secondary user;

forming a primary rule module customized to the primary user in a rule module clearinghouse stored in the computer system, the primary rule module associating at least one primary pattern data of the primary user with at least one primary execution command of the primary user;

forming a secondary rule module customized to the secondary user in the rule module clearinghouse stored in the computer system, the secondary rule module associating at least one secondary pattern data of the user with at least one secondary execution command of the secondary user;

subordinating the secondary rule module to the primary rule module;

comparing a bid biometric sample taken <u>via a biometric sensor</u> directly from the person of the secondary user with at least one previously registered biometric sample for producing either a successful or failed match;

determining that the secondary rule module is subordinated to the primary rule module; and

invoking the primary rule module of the primary user upon a successful match to execute at least one electronic transmission <u>from the computer system</u>.

64.   (Currently Amended) A computer system device for biometric processing of electronic transmissions, comprising:

a biometric input apparatus, for providing a bid or registration biometric sample of a user;

an electronic rule module clearinghouse, having at least one rule module including at least one pattern data of the user associated with at least one execution command of the user;

an electronic identicator, to compare at least one registration biometric sample stored in the electronic identicator with a bid biometric sample to produce either a successful or failed match; and

a command execution module, <u>responsive to a successful match</u> to invoke at least one execution command in the electronic rule module clearinghouse to execute an electronic transmission.

65.   (Previously Presented) The computer system of claim 64, wherein the electronic transmission is executed without the user presenting smartcards or magnetic swipe cards.

66.   (Previously Presented) The computer system of claim 64, further comprising:

storage for a plurality of registration biometric samples from a plurality of users; and

means for basketing a subset of the plurality of samples in the storage to facilitate the comparison with the bid biometric sample.

67.   (Currently Amended) The computer system of claim 64, wherein the electronic identicator is operative to compare at least one registration biometric sample stored in the electronic identicator with the bid biometric sample to produce either a successful or failed identification of the user <u>and upon a successful identification to invoke the execution command by locating the rule module customized to the user based on the identification</u>.

68.   (Previously Presented) The computer system of claim 64, wherein:

the execution command includes of one or more of the following: accessing stored electronic data customized to the user's rule modules, processing electronic data customized to the user's rule modules, and presentation of electronic data customized to the user's rule modules; and

the execution command for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

69.   (Previously Presented) The computer system of claim 64, wherein:

the pattern data includes one or more of the following: a user unique identification code, demographic information, an email address, a financial account, a secondary biometric, a non-financial data repository account, a telephone number, a mailing address, purchasing patterns, data on pre-paid accounts or memberships for products or services, electronic data usage patterns, employee status, job title, data on user behavior patterns, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, an instant messaging address, personal medical records, an electronic audio signature, and an electronic visual signature; and

the pattern data for the user is provided for the rule module by one or more of the following: the user, the electronic rule module clearinghouse, and an authorized third party.

70.   (Currently Amended) The computer system of claim 69, wherein the execution command for accessing stored electronic data includes permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products ~~like alcohol and tobacco~~; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

71.   (Currently Amended) The computer system of claim 64, wherein the execution command ~~for~~ includes accessing stored electronic data ~~includes~~ including permitting the user to access one or more of following data: insurance benefits; membership benefits; event admittance; electronic voting privileges for elections; electronic filing for taxes; privileges for permission to write checks; driver's license privileges; eligibility to purchase restricted products ~~like alcohol and tobacco~~; credit-rating and credit report accounts; and restricted portions of corporate intranet databases.

72.   (Previously Presented) The computer system of claim 64, wherein:

the pattern data includes demographic information of the user; and

the execution command includes accessing stored electronic data to determine eligibility to purchase restricted products or to access data or services.

73.-100. (Canceled)

101.   (Currently Amended)   A method for authorizing access to data at a third party Internet location, the method comprising:

receiving a biometric sample from a user at a terminal coupled to the Internet;

matching the biometric sample with a registered biometric of the user;

transmitting at least one access key to the terminal;

receiving a request to validate the at least one access key from the third party Internet location that has received a request from the terminal to access data residing at the third party Internet location;

confirming the validity of the at least one access key received from the request of the third party Internet location; and

transmitting to the third party Internet location the user's account access information relating to the third party Internet location, whereby the user is permitted to access data residing at the third party Internet location.

102.   (Currently Amended)   A biometric authentication method in a computer system for performing actions on data stored at a remote site, the method comprising

 a. receiving a biometric sample from a user <u>via a biometric sensor</u>;

 b. matching the biometric sample with a registered biometric of the user <u>stored in the computer system</u>;

 c. transmitting to a rule module clearinghouse component <u>stored in the computer system </u>a user identification code associated with the registered biometric of the user;

 d. identifying at the rule module clearinghouse component at least one rule module associated with the user identification code;

 e. extracting data <u>stored in the computer system </u>that is associated with the user and pertains to the least one rule module; and

 f. <u>the computer system </u>performing at least one action with the extracted data, such action defined by the rule module.